Montana Law Review

Volume 61
Issue 1 *Winter 2000*

Article 4

1-2000

Privacy in Cyberspace: Transcripts from the 1999 Judge James R. Browning Symposium

Jeff Renz
Moderator, jeff.renz@umontana.edu

James Harvey
Panelist

Larry Elison
Panelist

Nancy Sinclair
Panelist

Chris Tweeten
Panelist

See next page for additional authors

Follow this and additional works at: https://scholarworks.umt.edu/mlr

 Part of the Law Commons

Let us know how access to this document benefits you.

Recommended Citation

Jeff Renz, James Harvey, Larry Elison, Nancy Sinclair, Chris Tweeten, and Orson Swindle, *Privacy in Cyberspace: Transcripts from the 1999 Judge James R. Browning Symposium,* 61 Mont. L. Rev. (2000).
Available at: https://scholarworks.umt.edu/mlr/vol61/iss1/4

This Transcript is brought to you for free and open access by ScholarWorks at University of Montana. It has been accepted for inclusion in Montana Law Review by an authorized editor of ScholarWorks at University of Montana. For more information, please contact scholarworks@mso.umt.edu.

Privacy in Cyberspace: Transcripts from the 1999 Judge James R. Browning Symposium

Authors

Jeff Renz, James Harvey, Larry Elison, Nancy Sinclair, Chris Tweeten, and Orson Swindle

This transcript is available in Montana Law Review: https://scholarworks.umt.edu/mlr/vol61/iss1/4

PRIVACY IN CYBERSPACE[1]

Transcripts from the 1999 Judge James R. Browning Symposium

MODERATOR: *Jeff Renz*[2]

PANELISTS:[3] *James Harvey*[4]
Larry Elison
Nancy Sinclair
Chris Tweeten
Orson Swindle[5]

MR. RENZ: . . . .

The subject of the next panel is cyber privacy, or privacy on the Internet.

To give you a feel for the framework of the discussion, our court and other courts have talked about privacy aside from the Internet and essentially broken it down into two spheres. The first . . . is transactional privacy; that is, our right not to have other people or the government know what we happen to be engaging in at any particular moment. [The second is] . . . informational privacy; and that is our right to have other people or the government not know what it was we did the other day or collectively the last 365 days.

At some point, . . . transactional and informational privacy will overlap. On the Internet when we talk about transactional privacy, of course, we're talking about communications . . . .

In connection with the idea of privacy . . . there is the idea of security. The question of security brings up the question of encryption, and encryption's key in government's desire to regulate and, in some cases, prohibit encryption of Internet regulation.

---

1. All footnotes are attributable to the editors.
2. Professor of Law, University of Montana.
3. For an introduction of the panel members, please see Mr. Renz's descriptions, *infra*.
4. Please see Mr. Harvey's comments in the follow-up, Summer issue of the MONTANA LAW REVIEW, Volume 61, No. 2.
5. For an introduction to Orson Swindle, please see page 1 of this issue.

The tension that we see, then, is very much a tension between the public and the private sector. Some want government to be able to take control and protect our privacy. Others say mere governmental intervention will result in a compromise of privacy. Others say, the Internet, as we have heard many times, will take care of itself. There are many, many institutional, . . . financial, and . . . economic incentives for privacy on the Internet.

Currently, there is an Internet site, an Internet company called TRUSTe[6] . . . which gives out what they call trust marks. This company will certify that this Internet site takes certain steps to protect your privacy interests.

The Internet industry is developing certain protocols to ensure privacy of transactions. Of course, we don't want our Social Security numbers or our credit card numbers handed over to anybody who might want to be able to find them. We want means to ensure that when we send that credit number to an E-commerce company, that that is the only place it will go to and not to other people, and that people will not be able to break into that company's records and pull that number and other numbers out.

So the tension here is between governmental regulation in order to ensure privacy, and governmental intervention in order to breach privacy, and the private sector's attempt to regulate itself and to ensure the privacy of its users.

. . . .

With us . . . today is Nancy Sinclair.[7] Ms. Sinclair is an associate at James, Gray, Bronson & Swanberg, in Great Falls. Ms. Sinclair is a former Judge Advocate in the Navy . . . . [I]n her role as a Navy judge advocate, she . . . [advised] Navy authorities on signals intelligence operations, and has taken that expertise to James, Gray, Bronson & Swanberg, where she advises employers about e-mail and Internet privacy issues.

Larry Elison is with us today. Larry is a retired professor of law at the University of Montana Law School who has written extensively on areas of privacy. Professor Elison taught constitutional law and, when I was a student here, taught criminal law and procedure.

Finally, with us is Chris Tweeten. Chris Tweeten is the

6. <http://www.truste.org/>.

7. Nancy Sinclair is currently with the firm of Rebeck, Crum, & Sinclair in Great Falls, Montana.

chief counsel to the Attorney General of the State of Montana. He is a graduate of the University of Montana School of Law. He has been with the Attorney General almost since graduation, after clerking with Judge Jamison, with the exception of about a four-year stint in private practice. Chris Tweeten will speak to us about the concept and the role and . . . the novelty for Montana practitioners, county attorneys, and law enforcement people of the idea of obtaining information from data banks and information from computers.

Finally, last of all, . . . Commissioner Swindle[8] will comment upon the role of the private sector and . . . the state of affairs with respect to the private versus the public sector in protecting Internet privacy.

I am going to exercise a moderator's prerogative and change the order of speaking. We have heard from Jim Harvey[9] who has given us a wonderful overview of how privacy interests may be triggered in Internet transactions. We haven't heard much about privacy, itself, and sort of the underlying concept of the importance of privacy, and that's why I would like to start with Professor Elison.

MR. ELISON:

. . . .

The first thing, I'm overwhelmed. I don't understand what's going on. I am completely lost. I guess that's why I'm not teaching any longer. I'm retired, and I think it's a matter of obsolescence.

There is sort of a new life. It's like a virtual reality. It's not something I can touch and feel or act upon. And I was noticing a memo . . . which sort of indicates the obsolescence of all of us as teachers, and it was a memo to the Dean. It said, "Word has come down to the Dean that by use of a teaching machine, old Oedipus Rex could have learned about sex without ever disturbing the queen."

What's happening is something out there that is beyond all understanding. I think it's sort of a magical kingdom, something that's moved on. We're trying to put it into a context of something very concrete. How are we going to get money out of these people? Do we need money out of these people? Are they impacting the infrastructure of the entire system so that

8. *Supra* note 5.
9. *Supra* note 4.

they have to pay? And if so, how much, when, how?

Seems to me [that] it becomes almost an impossible jurisdictional morass. You heard the last speaker, and I was very impressed by his remarks, Mr. Harvey,[10] in terms of saying don't pass state laws. We really don't like the [European Union] (EU) regulatory scheme because it impacts on business in a very negative way, or could.

And what about federal law? Well, we're kind of concerned about federal law and we'll focus our debate on that.

Sounds to me like if you are going to get regulation, it has to be global in nature. Now, that's going to scare everybody a little bit, I assume. Like Mr. Swindle, I'm sort of a Libertarian also . . . .

. . . .

I used to be sort of a liberal Democrat, I guess, until practically all of their ideas were swallowed whole cloth by the Republican Party and for the worst of all possible reasons. I don't find a place left to go very much. And so maybe in my retiring and declining and deteriorating years I'll turn solely to a virtual reality and live on the Internet.

My current situation is that I don't get along with computers very well. I'm computer challenged. I'm Internet challenged. Is that the proper politically correct kind of term? And I'm certainly a non-aficionado, if that's the word, of Microsoft and Gates, and so I agree in that direction.

I have a kind of computer mantra that I live by, something like this: It seems to me that there are an infinite number of undetectable errors in the computer. I've also found that any given program, if running, is obsolete. Any given program costs more and takes longer than advertised. If a program is useful and works, it will be changed. Program complexity grows until it exceeds the capability of the program manager; and, finally, I found the most common program language is profanity.

The thing that I think I've learned most from this morning's presentation and this afternoon's beginning is that the computer Internet world is global and you have to deal with it on the basis of it being global.

Now, that having been said, I'm going to talk a little bit about the concept of privacy. And privacy, in terms of its development, is not global. It's something else.

Montana, for example, guarantees to its citizens more

10. *Supra* note 4.

privacy than perhaps any place else in the United States, if I'm reading the cases, the law, and the language correctly.[11] The Montana constitution specifically identifies privacy as not only, I think, a fundamental right, but a foundational right out of which most of our liberties may be seen to have evolved.[12]

And there are a couple of sides to that. [Mr. Renz] mentioned a couple. I'll approach it in a little different fashion. The two sides that I see in this foundational privacy is freedom from intrusion on one side. And I mean any kind of intrusion, and part of that goes on with the communication of information through the Internet after that intrusion has been made.

[T]he second side is freedom of choice. And our government, through a variety of regulatory schemes and criminal laws, limit our choices, and that limit on choices has expanded remarkably. Both of these things we have to be wary about and understand.

[P]rivacy actually developed from two sources, . . . as I see it, in the United States. The first source was sort of a common law development of privacy, an idea that was developed by a couple of notable writers, . . . Brandeis and Samuel Warren,[13] in an article, and then developed even more by one of our notable professors, Professor Dean Prosser,[14] notable in terms of the legal world.

And it was kind of a protectional idea for the dignity of the individual, and it was protected through the court system and tort law and it had four sides to it. One was a protection from intrusion into one's solitude.[15] Private affairs are your affairs, not somebody else's.

Second was public disclosure of private facts.[16]

The third was some kind of publicity placing one in a false light.[17] Not defamation, because it just placed you in a false light with publicity.

And the fourth one was the appropriation of one's name or

---

11. *See* Larry M. Elison and Dennis Nettik Simmons, *Right of Privacy*, 48 MONT. L. REV. 1, 17-19 (1987). *See also* Deborah E. Elison & Larry M. Elison, *Comments on Government Censorship and Secrecy*, 55 MONT. L. REV. 175 (1994); 5 Montana Constitutional Convention of 1971-1972, at 1671-79 (1979); MONT. CONST. Art II, § 10.

12. *See* MONT. CONST. art. II, § 10.

13. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

14. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

15. *See id.*

16. *See id.*

17. *See id.*

likeness for commercial benefit.[18]

This was the common law side of the development of privacy. There was another side that developed out of the constitutional premise that a person could be free from, usually, government intrusion.

It may have come out of the Fourth and Fifth Amendments to the Constitution, freedom from search and seizure, and freedom from self-incrimination.[19]

. . . .

[I]n the State of Montana we developed privacy in a . . . much broader sense. I'm reading from a case that was decided by the Montana Supreme Court in 1999. "Our conclusion is that the defendant in this case had a reasonable expectation of privacy buttressed by the fact that Montanans have a heightened expectation of privacy as evidenced by the specific provision given that right under Article 2, Section 10 of the Montana Constitution. We have consistently held that Montana's unique constitutional scheme affords citizens broader protection of the right to privacy than does the Fourth Amendment to the United States Constitution."[20]

If that be true, and maybe it's a little bit of self-congratulation in terms of what we're doing in Montana, what does that mean to the Internet, which is a global attack upon our individual privacy?

There are two more sides to it. The other two sides are the public and private side. You heard Mr. Harvey[21] speak about the accumulation, manipulation and distribution of information which we, as citizens using the Internet, generally volunteer . . . to corporate entities or to other individuals. We just give them that information.

And there has been substantial concern, so we are told, that the EU has a Data Directive which is going to regulate and protect the information that is accumulated on the Internet.[22]

There are a number of interesting problems. First, there is the creation, I am told, of something like data czars in fifteen

---

18. *See id.*

19. *See generally* Griswold v. Conneticut, 381 U.S. 479 (1965).

20. State v. Bassett, 294 Mont. 397, 340-341, 982 P.2d 410, 418 (1999). *See also* State v. Hubbel, 286 Mont. 200, 951 P.2d 971 (1997) and State v. Siegal, 281 Mont. 250, 934 P.2d 176 (1997) (overruled on other grounds).

21. *Supra* note 4.

22. *See* James Harvey, *An Overview of the European Union's Personal Data Directive*, 15 NO. 10 COMPUTER LAW. 19 (1998).

different nations.[23] I like those kinds of terms. Like the war on drugs and, suddenly, all the constitutional issues that I hold dear are thrown out the window because, one, we've got a war and, two, we've got a czar.

In any event, I don't feel that I am protected in the least when I go on the Internet. So I'm going to do what I think Mr. Harvey[24] was suggesting we do. I'm going to have to maintain a personal kind of vigilance if I want to protect my privacy when I hit the Internet. I don't think there is any other way at the moment.

Nobody is going to be out there protecting me. I don't think the EU and the data czars will protect me. I very much doubt that the federal government will protect me. In fact, they are the most frightening aspect of the whole thing. They want to limit my ability to encrypt, to keep anything private. They want to put chips into computers so that they can see exactly what I'm doing, and that . . . comes as close to thought control as anything I can imagine. I do use my computer sometimes, just sort of meandering and thinking, et cetera. I don't know what the hell happens. If people can get into the computer, I'm very uncomfortable, really unhappy, and I think it's the maximum kind of invasion of my privacy.

Who is going to do it? Well, I can think of a lot of people that might be interested. I don't perceive myself, even if I'm a bit Libertarian, to be necessarily antisocial or criminally inclined, but I do fear the NSA and DEA and the FBI and the CIA and whatever other kind of agencies that you can put together, that they want to know everything because they have . . . big concerns.

They have . . . concerns about treason, and they have . . . concerns about terrorists, and they have . . . concerns about drug pushers. They want to tax the pharmacy companies that are pushing those good drugs, like Prozac and Viagra, et cetera. They want to get the money out of that side of it.

And then they want to hit the drug pushers on the other side that are actually supported by two independent groups pushing hard against each other: One, the DEA on one side and . . . the criminal syndicate on the other side. There is a big fight and there is a lot of money that keeps springing out of the fight. Very effective.

---

23. *See id.*

24. *Supra* note 4.

But the government needs that information if they are going to be effective against the war on drugs. They need that information if they are going to be effective against the terrorists that are everywhere to be seen.

Does that mean that in the process of gathering that information I have to forfeit my privacy as a citizen of the United States? It scares the hell out of me. I'm not sure. At this time I don't know. And since I'm computer challenged, I don't feel very comfortable by what people are telling me, "We've got it all taken care of, there is good security." How do they enforce it? I have not the foggiest.

I know the 15-year-old hackers usually can find an awful lot on the Internet, encrypted or otherwise.

I'm going to give you an idea, I think, of some of the problems that we're encountering. We know there are going to be criminal investigations because there will be exchange of information between organized criminals and there will be exchange of information among not-so-organized criminals.

There will be a variety of problems that have already arrived on the Internet, such as stalking, molestation, the commercial scams, conspiracies, hot stock, organized crime and now gambling. Gambling is a big item coming up on the Internet . . . . It has intriguing possibilities in a lot of ways.

Then there are the other sides, separate and apart from the criminal aspect, and that has already been mentioned, but there are going to be credit checks. And you are turning in your bank account, all that information, so there will be credit checks and, suddenly, you don't get good credit anymore.

I will depart just briefly [with] one anecdote. When I was struggling to get through law school in Washington, D.C., one time and ran out of money, I went to night school and worked for the Retail Credit Association to gather information, credit check kind of information.

Well, they almost got rid of me because I couldn't keep up. I couldn't do my work properly.

Most of the information that was being gathered was dry land. That means you didn't go out and investigate. You had telephone directories; you called somebody; you wrote the information down, probably no crosschecks.

The company got paid per case report. They wanted lots of case reports out of their employees, and the most damnable information was going into those reports that you can ever imagine. It could say this person is fifteen years old, lives at

such and such an address and has had three juvenile offenses. It was a female thirty-five years old, and that all goes into the report.

Now the question is, how do you get it out? It's going to be archived, Mr. Harvey, forever?

MR. HARVEY: Roughly speaking.[25]

MR. ELISON: Roughly, okay. You have employment evaluations that are going on there, I would imagine, apart from the commercial sales. You have political support, personal political attacks. You have proselytizing by cults and mainstream religions, and it's just mind boggling. I don't have any of the answers. I only have a lot of the concerns. Schizophrenic? Yes. Completely and totally.

So I think the main recourse for all of us is to be personally vigilant. [M]ost people that turn on that Internet system and see something come up, they believe it. It's true.

And a simple question is asked: Put in your name and your Social Security number. The general response, you put in your name and your Social Security number. You are talking about people that are going to be vigilant. I imagine they are going to be less than one percent of the total population using the Internet . . . .

I think the Internet also has kind of a hypnotic charm. It's like the Jungle Boy-snake, "Trust in me." You do. You just put the stuff in there and they feed it; they massage it; they distribute it; and I'm afraid many times [that] it's not accurate. Many times it's going to be used for a purpose not intended and not explained.

I have a little story I've mentioned before, but I think it really hits at the core of the problem that we're seeing. The story is about a banquet attended by our now Democratic presidential candidate Bill Bradley. During the course of the banquet, the serving person comes by and Bill Bradley taps him and says, "Could I have a couple extra cubes of butter?" Serving person says, "No." Bill said, "Well, hold on, do you know who I am? You know, I've been a senator and I've been a national NBA champion basketball player, and I'm now running for the presidency of the United States." And the serving person said, "You know who I am?"

25. *Supra* note 4.

"No, I don't know who you are."

"I'm the person in charge of the butter."

And what we're looking at now, and what I think we should be looking at is who has the power. I think the whole process of the Internet is just scaring to death the people that are presently in control. They don't know how to control what's happening anymore, so half a dozen laws are passed in the United States Congress. We have the EU Data Directive and we have people arguing, well, leave it up to private business. They will take care of it; they will be self-regulators. I've never seen a good self-regulator, but I like the idea better than Congress regulating. I don't know what's going to happen, and I think the real fear is we, the controllers, whoever "we" are, don't know where the power source is. We don't know where the power locus is. And if we don't know where the power locus is, we're going to have one very difficult time controlling the thing. And that's all I have to say. Thank you.

MR. RENZ: Professor Elison touched on a couple of things that brings up our next speaker, and that has to do with exchange of information among criminals and the actual commission of crimes on the net. [These include] such things as pornography on the net, cyber stalking, a crime that I just recently heard about, illegal gaming, identity theft and other data theft.

So we will now hear from Chris Tweeten as to, at least, state and local government approaches.

MR. TWEETEN: Thank you, Jeff. I want to thank the *Montana Law Review* for the opportunity to sit on this panel. If I might be allowed a personal aside, it's a real privilege to be on this panel with Larry Elison. It takes me back to those days, years ago, when I sat in his criminal procedure class upstairs and learned everything there was to know about the law of criminal procedure. It's really a privilege to be here on a panel with Professor Elison and all these other distinguished guests.

[B]efore I talk about those ways in which the criminal justice system seeks to pry into all of that private information that you think you have on your computer at home, I would like to remind folks that the Montana Legislature has done primarily what the legislature does best, that is, they have identified that there is a problem and passed a law. The problem that they identified is that there is the capacity for

others to misuse your computer system .... Since 1991, we have had a law on the books in Montana that has made it a felony to engage in certain kinds of illegal conduct with respect to someone else's computer.[26]

This statute, which is called Unlawful Use of a Computer,[27] which is a very creative name, deals with situations that we commonly know as hacking. That is, somebody else from the outside getting into your computer and either altering or destroying one of your software programs; or getting in your computer and stealing information; or getting into your computer and using it as a tool for acquiring any other property or thing of value without the consent of the owner.

These statutes have been on the books since 1991 .... They have not been frequently enforced in Montana as of yet. There are no reported cases in which the Montana Supreme Court has dealt with charges that have been brought under any of these statutes and, as a result, we don't really know exactly how effective they can be in dealing with the problems of other people getting unauthorized access to the information that's on your computer.

One section or subsection of that statute makes it illegal for anybody to obtain the unauthorized use of someone else's computer.[28] I wonder if the Internet sites, when they stash those little Cookies on your computer, could be challenged as making unauthorized use of your computer in violation of the statute.

Again, that's a claim that's not been brought in Montana or anywhere else that I'm aware of. But I think it certainly raises an interesting question about whether it's legitimate for an Internet Service Provider or some Internet company to assume that just because you visited their web site, that they have your permission to then stash data on the hard drive of your computer and call it up the next time you drop by and pay a visit.

....

One other thing that the Legislature has recently done in 1999 is to amend the statute on Privacy in Communications.[29] That's the statute that makes it illegal to tape record telephone conversations or otherwise wire tap somebody without their

26. *See* MONT. CODE ANN. § 45-6-311 (1999).
27. *See id.*
28. *See* MONT. CODE ANN. § 45-6-311(1)(a) (1999).
29. *See* MONT. CODE ANN. § 45-8-213 (1999).

consent.

In 1999, the Legislature added some language to that statute to make it unlawful to intercept a voice or data transmission on a telephone.[30] Since most computer modems that transfer information between computer systems operate over telephone lines, I think an argument could certainly be made, and I think the Legislature probably intended, that the unconsented interception of data being transmitted from one computer to another over a telephone line would be a violation of that statute. That statute just went into effect a couple of weeks ago and there have been no cases brought under it.[31]

But it illustrates a point that I think is significant. In Montana, we are in so many areas dealing with technology behind the curve with the rest of the country. If you have been following the debate about economic development in Montana, you've heard probably that one of the things that's standing as an obstacle to Montana joining in all of the prosperity that exists in the United States today as a result of the information age, is the backward nature of Montana's information infrastructure. So it shouldn't come as any surprise that our legal framework is as far behind the times as our technological framework.

Our Legislature has not traditionally been proactive in getting ahead of the curve on some of these issues and, as a result, we have large areas of Montana law in which use of computers and use of the Internet and transmission of data between computers is largely unregulated by state law.

[T]here are probably good reasons for the states to tread lightly in [this] area of regulat[ion] . . . given the global and national nature of commerce over the Internet and the problems that arise as a result of a patchwork of state regulations that may not be consistent with each other.

But I think it's certainly inevitable that as time goes by, the Montana Legislature is going to do what it does, which is identify problems and pass laws that it thinks will address them. I think it's inevitable that some of these laws will regulate in these areas as time goes by.

Now, talking about the subject of law enforcement as it deals with the access to private information in computers.

30. *See* MONT. CODE ANN. § 45-8-213(2) (1999).

31. *See id.* (amendment effective October 1, 1999).

Again, this is an area where Montana is somewhat behind the curve. There are no reported cases in Montana where the Montana Supreme Court has talked about the utilization of the primary tools that are available to law enforcement to gain information when that information is either a computer itself, or is information located on the computer. We have no indications in Montana on point at this time. Again, I think it's inevitable that those cases will come. And, frankly, I'm excited at the idea of what the Montana Supreme Court is going to do on some of these very complicated and difficult issues in which they are going to have to take existing principles of constitutional and common law dealing with criminal procedure and try to adapt them to this very complex and fast changing technology that exists with respect to computers and the Internet.

We do have two separate kinds of tools that are available to law enforcement in this area, and they are traditional tools. They are not new tools that have been designed for the Internet, but they are traditionally existing tools that are being adapted, I think, in the appropriate cases for securing access to computerized information or access to computers themselves, and those are investigative subpoenas and search warrants.

Investigative subpoenas have been in use in Montana for many years. They differ from search warrants in a couple of significant respects. One, they are purely creatures of statute;[32] that is, they don't have an anchor in the constitution like search warrants do.[33]

Second, they are generally directed at persons who are not suspects but, rather, . . . third parties that may have information that may be useful to law enforcement in investigating and prosecuting crime.

Traditionally, they have been used to secure access to things like electrical bills, telephone bills, [and] medical records in the hands of medical providers. They have been very effective for law enforcement in getting access to that kind of information.

Now, in Montana, the usefulness of these tools have been affected, as Professor Elison pointed out, by the existence of Montana's constitutional right to privacy.[34] This is an area in which the Supreme Court, I think, has been extremely active and extremely vocal and which they have, in some respects, [not

32. *See* MONT. CODE ANN. 46-4-301 (1999).
33. *See* MONT. CONST. art II, § 11.
34. *See* MONT. CONST. art II, § 10.

been] entirely consistent in the way that they approach the applicability of our right to privacy with respect to criminal investigative procedures.

The Supreme Court has, I think, firmly established its view that the Montana right to privacy [clause] affects the ability of law enforcement to make use of tools like investigative subpoenas and search warrants. There are numerous cases in which they vocalized their intention that the Montana right to privacy [clause] play a role in a court's decision as to whether a search warrant was properly exercised or whether an investigative subpoena was properly issued.[35]

In 1997, the [Montana Supreme] Court issued a decision that clarified its view as to the interface between investigative subpoenas and the Montana right to privacy [clause]. That case was *State v. Nelson* . . . .[36]

James Nelson was involved in an automobile accident in which he smacked a guardrail in Dawson County and ended up going to the hospital and having some medical procedures done, one of which was a blood alcohol test.[37] [T]he doctor who was treating him was struck by the fact that he was receiving some medical treatment that ordinarily would have been expected to cause him some physical discomfort and he seemed to be quite immune from any physical discomfort that was being imposed on him by the medical procedures . . . .[38]

So the doctor felt that, for therapeutic reasons, it was important to get an evaluation of this person's blood alcohol level. So that blood test was taken.

The law enforcement officers became aware of the fact that blood was taken in the hospital and they secured an investigative subpoena directed at the hospital emergency room records to try to get access to [records showing] . . . this suspect's blood alcohol level . . . at the time he was checked into the emergency room.[39]

The investigative subpoena issued. They acquired the information, got the conviction, and that was then appealed to the Montana Supreme Court.[40]

---

35. *See* State v. Nelson, 283 Mont. 231, 941 P.2d 441 (1997); State v. Dolan, 283 Mont. 245, 940 P.2d 436 (1997).

36. 283 Mont. 231, 941 P.2d 441 (1997).

37. *See id.* at 234, 941 P.2d at 443.

38. *See id.*

39. *See id.* at 234, 941 P.2d at 444.

40. *See id.* at 234-235, P.2d at 444.

In that case, the argument was made that the issuance of an investigative subpoena, without complying with some showing that a crime had been committed and that the medical records were important evidence of the crime, violated Article 2, Section 10, of the Montana Constitution.[41]

The Montana Supreme Court basically agreed with Nelson's allegation that [this] was the law in Montana but, nevertheless, affirmed his conviction because they found that the information that was presented to the Court in support of the investigative subpoena, by itself, was sufficient to establish probable cause to believe that a crime had been committed and that these medical records would be evidence that would be useful in the prosecution of that crime.[42]

The Court's essentially conflated together the compelling state interest test in Article 2, Section 10, of the Constitution with the probable cause standard that exists in Article 2, Section 11, the section that governs searches and seizures.[43] [The Court] held that in order to issue an investigative subpoena seeking the production of what the court referred to as constitutionally protected information, which is a category that I think bears some further definition in future cases, the parties seeking the subpoena would have to make a showing, essentially, of probable cause that would be the equivalent of what they would have to show to get a search warrant.[44]

So with respect to whatever "constitutionally protected information" means, the Montana Supreme Court has said that an investigative subpoena and a search warrant are essentially the same thing.[45]

The *Nelson* holding has been written into statute in the 1999 Legislature in an amendment that was adopted to the statute governing investigative subpoenas. So there is now a statutory basis for the requirement that probable cause be shown before investigative subpoenas can be issued to find constitutionally protected information.[46]

I think this holding has some interesting implications for the issue of access to computerized information, because some of the computerized information that law enforcement will want to

41. *See id.* at 231, P.2d at 446.
42. *See* State v. Nelson, 283 Mont. 231, 244, 941 P.2d 441, 450 (1997).
43. *See id.* at 243-244, 941 P.2d at 449-450.
44. *Id.*
45. *Id.*
46. *See* MONT. CODE ANN. § 46-4-301 (1999).

get in a criminal investigation is likely to be information that's in the hands of a third party and not in the hands of a suspect or in a suspect's computer.

You heard Mr. Harvey[47] talk about the various kinds of fingerprints that Internet users leave when they visit an Internet site. A lot of those fingerprints are going to be very useful information for law enforcement in trying to make cases in certain kinds of crimes that are accomplished using computers.

For example, one of the most frequent uses of computers for criminal behavior in the United States involves the solicitation of minors for sexual activity through the Internet. The way this works is that an adult offender will go into an Internet chat room in which he has reason to believe, or she has reason to believe, minors will be present. And using an assumed identity, as people ordinarily do when in chat rooms, will try to solicit interested minors to either give them information, provide them with photographs or, in some cases, to even meet for the purposes of engaging in sexual conduct.

This is a violation of federal law.[48] It is also a violation of state law in Montana[49] to engage in that kind of conduct. One of the ways that law enforcement agencies traditionally try to ferret out this kind of conduct is by engaging in undercover sting operations in which law enforcement officers will pose as interested minors and will go into these chat rooms and engage in these exchanges of information with the offenders who are interested in trying to solicit minors for sexual conduct. [They will] try to get these offenders to agree to meet with them at a certain time and certain place, at which time they meet with the offender and arrest the offender for violation of laws dealing with soliciting minors for sexual conduct.

Records that are kept, as Mr. Harvey[50] indicated, by the Internet sites are very useful in trying to make these cases because one of the things that law enforcement has to show in order to prove these crimes is that the offender was actually using a computer and engaging in this kind of conduct in this chat room on this particular date.

Some of those fingerprints that he discussed[51] that are left

47. *Supra* note 4.
48. *See* 18 U.S.C. § 2251 (1999).
49. *See* MONT. CODE ANN. § 45-5-625 (1999).
50. *Supra* note 4.
51. *Id.*

when the offenders make use of these sites are very useful. And so investigative subpoenas are frequently used to try to get that information from the Internet Service Providers [and] from the Internet sites to try to help make those cases.

The question arises in Montana as to whether that information is, in fact, constitutionally protected. So that the investigative officers would need to essentially meet search warrant standards before they would be entitled to the issuance of an investigative subpoena to get at that information.

There are no cases in Montana on that point, but there are analogous cases in Montana dealing with access to telephone and electrical bill records that would tend to suggest that these kinds of commercial records that are kept by third parties who provide services to individuals are not records in which any reasonable expectation of privacy exists.[52]

I think the argument certainly can be made that an analogy exists between telephone and electrical billing records on the one hand and the kind of electronic fingerprints that are left in these Internet sites on the other, and that law enforcement ought to be able to get access to that information through an investigative subpoena without first having to establish probable cause to believe that this defendant has in fact engaged in the activity that would constitute a crime.

The other major tool that's available to law enforcement is the search warrant, on which there is a large body of case law in Montana. I don't think I've got the time to go through a lot of discussion about search warrants, but I think it is important to understand that the use of search warrants to seize computers or computer data presents some interesting practical problems for law enforcement.

A computer and computer data can be the subject of a search warrant for a couple of different reasons. The computer can, itself, be an instrumentality of the crime; that is, it may be something that the offender used in the commission of a crime itself. Or, the computer may just be a repository of information that is, in itself, evidence of a crime. It might be analogous to a file cabinet in that respect, where documents are kept that might be evidence of a crime.

Because of the unique technological nature of computers and computer systems, law enforcement needs to have access to

52. *See* State v. Dolan, 283 Mont. 245, 256, 940 P.2d 436, 442 (1997) (citing Hastletter v. Behan, 196 Mont. 280, 283, 639 P.2d 510, 511 (1982)).

some very specialized expert knowledge about computer systems and about how computers work in order to make use of search warrants to seize computers and to get data off of computers.

Computers are very sensitive, first of all, as a matter of hardware, to things like dust, static, other environmental factors that make the corruption of data in a computer a real problem for law enforcement if they don't know what they are doing when they are dealing with the computer system itself.

Beyond that, in going into the computer and trying to secure access to information, the officers need to have access and expertise in order to know what to look for and how to find it in the computer system.

There has been litigation in other states, there hasn't been in Montana, over the subject of whether law enforcement officers are authorized by law to bring along outside experts with them when they execute a search warrant or to use the knowledge and opinion of outside experts in establishing probable cause for the issue of search warrants.[53]

Courts have generally been holding that it is legitimate for law enforcement to make use of specialized knowledge of outside experts in making an application for a search warrant and filling out the affidavit for a search warrant in order to establish probable cause for the issuance of the warrant; and then, in going to the site in executing the warrant, making use of the assistance of computer experts in order to make sure that, first of all, they don't corrupt the data that they are looking for; secondly, that they don't inadvertently damage the equipment; third, that they don't inadvertently exceed the scope of the warrant.[54]

The use of outside experts, I think, can be very helpful to law enforcement in all three of those aspects in making sure that they comply with the rules that exist with respect to issuance of search warrants for this particular kind of evidence.

There is an interesting issue with respect to computers in the execution of search warrants, which is whether it's preferable for a law enforcement officer to basically inventory the contents of the computer on site or to dismantle it, take it to a remote and secure location and then conduct their inventory search at that point.

---

53. *See* People v. Superior Court, 104 Cal. App. 3d (1980); Schalk v. State, 767 S.W.2d 441 (Tex. App. 1988); U.S. v. Schwimmer, 692 F. Supp. 119 (E.D.N.Y. 1988); Florida v. Wade, 544 So.2d 1028 (Fla. Dist. Ct. App. 1989).

54. *See generally id.*

There are a couple of factors that pull in opposite directions in terms of making that decision as to whether one or the other of those alternatives is preferable. On the one hand, given the nature of computer systems, law enforcement officers have to be vigilant to the possibility that somebody in a remote location may get access to the computer while the officer is in the room executing the search warrant and either alter, corrupt or destroy data that may be located in that computer. The nature of computers is such that that sort of contact is possible . . . as long as the computer is still networked and plugged into its modem and in its original configuration . . . .

Cutting against that is the fact that I mentioned before, which is the possibility that law enforcement officers may inadvertently, in the process of dismantling and reassembling the computer, corrupt data, destroy data, or make errors in the reconfiguration which may make it impossible to retrieve data off of the computer.

For all of those reasons law enforcement officers, I think, are trained to make sure that they have access to the technical expertise that they need to assist them in the execution of the warrant, in planning the search initially and, also, in executing the warrant as time goes by and [when] they are actually going into the place and serving the warrant.

One other issue that I want to touch on briefly is the protection that exists for certain kinds of computer data under federal law. There is a statute called the Privacy Protection Act[55] that was enacted some years ago by Congress that specifically exempts from searches and seizures by state and federal law enforcement agencies data that is assembled by someone for the purposes of publishing, or documentary evidence that is used by somebody to assemble an article or other thing that the person intends to publish.[56]

This statute has obvious implications for serving search warrants and investigative subpoenas on computers by state officers and also by federal officers because, frequently, claims will be made that the offender, who is the target of the search warrant, has the intention to publish something that's on his computer. The argument will be made that in the course of executing the warrant, the officers got into some of this publishable material and violated the Privacy Protection Act in

55. *See* Privacy Protection Act of 1980, 42 U.S.C. § 2000aa.

56. *See* 42 U.S.C. § 2000aa-6(a) (1980).

the process.

One saving grace is that Congress specifically provided that there is no exclusionary remedy for violations of this statute, that is, the exclusionary rule doesn't apply to evidence seized in violation of the Privacy Protection Act.[57] But there is a pretty clear civil remedy[58] that's provided in Congress, and it raises some very serious implications for the law enforcement as they engage in the execution of these search warrants.

[T]here is a fair body of case law that is developing under the Privacy Protection Act in terms of claims that are being made in the search and seizure context about violations of the statute.[59] It's something that law enforcement officers need to be familiar with and need to be very careful about to avoid becoming the targets of litigation themselves.

. . . .

MR. RENZ: Along with governmental intervention, governmental desire to gather information about us, of course, another level is our employer's desire to know something about us and especially what we're doing in the workplace.

So, without further introduction, I think I'll just simply turn that over to Nancy Sinclair.

MS. SINCLAIR: Thank you. We have heard a lot today about our privacy when we get on the Internet as an individual, but many of us are using a computer and hopping on the Internet from our workplace and the computer belongs to an employer. We're also using, maybe, an interoffice-type LAN, local area network, or a WAN, a wide area network, and these are all things that belong to our employer. How does the expectation of privacy in that situation change?

What I'm going to try and do today is just hit some of the things that we would advise an employer who calls us to consider and maybe some policy changes and other things that they would want to implement in order to let their employees know what their expectation of privacy would be.

Just so you have a context of how this would work, we get calls from employers who really have not given any of these

57. *See* 42 U.S.C. § 2000aa-6(e) (1980).

58. *See* 42 U.S.C. § 2000aa (1980).

59. *See, e.g.*, Citicasters Inc. v. McCaskill, 883 F. Supp. 1282 (W.D. Mo. 1995) rev'd, 89 F.3d 1350 (8th Cir. 1996).

issues any thought or even the issue of privacy, and we hear: "My former employee downloaded files and took them with him to a new job and it had proprietary information," or something of that nature. "What do I do?"

In order to avoid getting to that point, . . . an employer has to look at their office policies. Many of us, even as lawyers when we are employed by a law firm, receive an employment manual and in there it talks about the different office policies and what you can expect.

One of those things that should be addressed in that policy is: What is the expectation of privacy of an employee on their computer? That includes the computer hard drive; that includes any files that they may have stored on the server; that includes their use of the Internet from the company via the company access.

An employee expectation of privacy is usually looked at in terms of . . . the context of the employment relationship. Normally, courts hold that an employee has a lesser expectation of privacy in the workplace and [that the employee's] expectation is based upon . . . the openness of the workplace.[60] [D]o you share a desk? Do you have an individual office? Do you lock your filing cabinet?

When you look at this in the electronic age . . . [the issues include]: Where does your computer sit? Who has access to it? Can other employees remotely access your hard drive; remotely access your files sitting on the server? What files are password protected? Are any of your files password protected? [A]ll of those things need to be considered when formulating a privacy policy in the workplace.

In addition to that, there has been a lot of discussion about the criminal statutes and what's acceptable; what's not; the constitutional provisions of privacy; and then there [are] employment statutes.

We have seen questions of employers wanting an accounting of the digital information that was taken by a former employee. How do you force that employee to say, I took X, Y, Z files and I took them in a certain format?

---

60. *See, e.g.*, Medical Lab. Management Consultants v. American Broad. Co., Inc., 30 F. Supp. 1182, 1188 (D. Ariz. 1998); Ali v. Douglas Cable Communications, 929 F. Supp. 1362, 1382 (D. Kan. 1996); People For the Ethical Treatment of Animals v. Bobby Berosini, Ltd., 895 P.2d 1269, 1281 (Nev. 1995) ("there is, generally speaking, a reduced objective expectation of privacy in the workplace."); Cox v. Hatch, 761 P.2d 556, 563 (Utah 1998) (no reasonable expectation of privacy in a "common workplace").

Montana has a statute, . . . [which] talks about what belongs to an employer.[61] It does not in any way address electronic media, but we have used that to say those files belong to the employer and under an additional statute,[62] we were entitled to an accounting of what files were taken.

So when it comes time to address privacy within the work area, an important thing to remember is in many places the computer acts as an electronic filing cabinet. It also acts as an interoffice memo system and a way of interoffice communication. So you need to think of all those things and determine what sort of privacy you want to grant your employees.

Probably the biggest problem is many employers, after that, determine that they want to give their employees a written policy that says: "You have no expectation of privacy within the workplace, including our computer, our computer system [and] any data stored on there [or] retrieved from. Anything belongs to us, it's not yours, and you have no expectation of privacy in it."

The problem . . . arises when you have supervisors or other individuals who have their own little policies within a department or a division that do create expectations of privacy in the workplace in the employer's computer.

Many companies [and] firms . . . [now] have access . . . to e-mail from outside sources. A frequently asked question is, can I read an employee's e-mail? Nationally, there is a trend toward saying, in the private sector, there is no expectation of privacy in e-mail received on an employer's computer.[63]

The thing about Montana is, as Professor Elison discussed, we have a heightened constitutional privacy provision.[64] I believe that the Montana Supreme Court could easily find that employees do have an expectation of privacy in their e-mail, especially in light of the fact that many companies don't have any policies even addressing this issue.

What do you do, then, as an employer to remedy some of these situations? You can do the privacy policy, but you can take it a step further, . . . implementing what is called a computer user agreement. This is an agreement that your

61. *See* MONT. CODE ANN. § 39-2-102 (1999).

62. *See* MONT. CODE ANN. § 39-2-407 (1999).

63. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (holding that once the employee communicated over an e-mail system which was utilized by the entire company, any reasonable expectation of privacy was lost).

64. *See* MONT. CONST. art. II, § 10.

employees would sign at the time of employment or at the time they are given access to the company computer and all the systems that it is hooked up to.

[T]he user agreement . . . acknowledges in writing, with a signature, that the employee understands that they are being given access to the employer's computer system but all the information contained in, generated on, [and] sent over is the property of the employer.

It also specifically spells out that there is no expectation of privacy in any file [or] database, including data stored on the individual computer, the hard drive, the network, the server, or a disk or received on or stored in an employer Internet account.

It goes farther to say that the employee acknowledges that the system may be monitored for lawful purposes. A lawful purpose would be a system administrator monitoring the system to ensure that e-mails are being delivered properly in a timely fashion and that there is a free flow of information.

If you are giving your employees access to a specific type program and allowing them to take it home and place it on their home computer, you need to address in this user agreement the limitations on them using that program.[65]

An example would be . . . in engineering and architectural type arenas [where] there is a generic CAD program, which is a drawing program, and many of these individuals take it home and are able to work on projects . . . in their home environment. They are given that program for a limited purpose by the employer, and the employer needs to spell that out so that there is no question.

The other thing that you need to address is if you are giving your employees access to the Internet, you need to tell them what they can do on the Internet, what expectations you have.

You need to tell them what types of sites are prohibited if you are going to prohibit any sites. You need to tell them whether they can only use the account to access the Internet from their work computer or [whether they] are they able to use the access from their home computer? You also need to tell them that if they are violating any federal laws while they are on the Internet, that that could result in some sort of disciplinary action, up to and including possible termination.

---

65. For an example of a model user agreement regarding at home use of software by an employee and an employee's access to the employer's internet account from home, see the general model user agreement provided by the Attorneys Liability Protection Society. <http://www.alps.org/library.htm>.

And, really, you need to tell them that any violation of the user agreement could result in disciplinary action, up to and including termination.

It's difficult in the employment relationship area because many employees somehow don't think of their computer in the same context as a desk, a filing cabinet or anything like that, and it's up to the employer to clearly state to their employees what their expectations are and what a violation of company policy could result in.

MR. RENZ: We have heard from the Attorney General and we have heard from counsel for the employer.

I next want to turn to Orson Swindle. By way of introduction, I read the other day something about cooperative filtering. The idea of cooperative filtering . . . sort of demonstrates why and how obtaining or turning over information about yourself to an Internet company can actually inure to your benefit.

The idea of cooperative filtering is, I can go to something like Amazon.com and give them a list of books that I have read recently and they will take that list and they will match me up with other like people who have read the same kinds of books. And then I can report in[to Amazon.com] and these people can report in[to Amazon.com] in the future and say, "Well, I just read this new book and I liked it very much." And that information can then be passed on to other members of the group. It's like going to your local bookstore, which of course is becoming obsolete, as we know, and asking your bookstore owner, "Well, what do you recommend today?" And [he or she] would say to you, "Well, Jeff, I know what your interests are and I would recommend this."

Now, I receive a recommendation from some human being somewhere in the world who I don't know but who apparently has the same kind of tastes that I do.

The other thing that we note is that the prospect and the idea of legislating for privacy is based upon a key assumption, and that assumption is that we know what the architecture and what the landscape is going to look like in the future. That might be true with some technologies but we certainly know it is not necessarily true about the Internet and about computer technology.

Now, I will ask Orson Swindle to pass on his comments about the benefit or lack of benefit of governmental regulation

for privacy.

MR. SWINDLE: Thank you very much. To my Libertarian professor friend, I could not help but thinking and you recalling that years ago you were a Democrat and a liberal, and I think it was Winston Churchill who once said, "If you weren't a liberal when you are young, you had no heart and if you weren't a conservative when you are old, you had no brain." So we're making progress.

Speaking of cooperative filtering, that thing with the books, if anybody is interested, to show you that my life is an open book, I've recently read *Modern Machiavelli* by David Ledeen and *A Man in Full* by Tom Wolfe, and I have read John McCain's book which I had a little bit to do with writing—not writing, but editing.

But, this matter of privacy is just an extraordinary thing. And, we at the Federal Trade Commission are working with it constantly. It is a big issue. If you were tuned in early in the summer, it was the hottest topic in the political circle, quite a buzzword. And every politician, before they went home on recess, wanted to be in the game, establishing a position that was for God, country, apple pie and mom's homemade cooking and everything.

But not to make light of it, I had the occasion about a year ago to meet Scott McNealy who is the CEO, owner/founder, as I recall, of Sun Microsystems who are arch adversaries of Bill Gates and Microsoft, as I remember the story.

Scott McNealy, fascinating guy, he came into the meeting. I was in a typical Washington, D.C. suit. I was out on his grounds in Silicon Valley. He came in jeans, Weejuns and a pullover sweater. And I said, "Hi, Scott, I'm Orson Swindle, how about a cup of coffee?" And he said, "We call it Java around here." If you know anything about Sun Microsystems, that's their operating system.

He gave a speech a few weeks later, . . . and he said, "Privacy, forget about it. There is none." And as blunt as he was, and he does tend to be blunt, I really like the guy, he's right. It's just incredible the age that we live in and the things that can be done through communication systems, and computers in particular.

The Federal Trade Commission, I think we just celebrated

our 100th case[66] having to do with the Internet, and a number of those are on identity theft,[67] database manipulation and use of information that has been gained surreptitiously by large companies, credit organizations, credit reporting organizations, big-time stuff. And it is just mind boggling the expanse to which this all goes.

It's almost as if the train left the station, and we're now trying to figure out how to get on board and do something about it, and it's highly questionable whether we can. As the professor said, it really gets down, in most cases, . . . not in all cases, to protecting yourself.

The government is going to have a very difficult time doing this, protecting the consumers, and it raises a number of very critical issues.

One is, there is a huge collection of people out there in the privacy world, if you will, Advocates for Privacy, that are urging the government to regulate. We had a big debate, as I said, earlier in the summer, as to whether we would regulate, . . . I think Jim[68] mentioned, with some of his slide presentations, the FTC's survey on privacy policies, whether people (web sites) had them or not. We did the first survey in the spring of March of 1998,[69] as I recall.

One of the figures . . . was [that] sixty-seven percent of corporations, commercial web sites, have a privacy statement . . . .[70]

That only answers one question: Do they have one? Is it posted? It tells you nothing about the content of that privacy policy. It just says: We've got one; if you want to look, here it is, and you judge the quality yourself.

The year prior to that, the survey [Jim][71] was mentioning, the one we just finished in the spring of [19]99[72]—it was a

66. *See* <http://www.ftc.gov/opa/1999/9910/fyi991029.htm>.

67. *See* Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998). *See also* FTC Report to Congress: Individual Reference Services, December 1997 at 13-16. *Also see* FTC, ID Theft: When Bad Things Happen To Your Good Name. <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm>. *See also* <http://www.consumer.gov/idtheft/>.

68. *Supra* note 4.

69. *See* FTC, Privacy Online: A Report to Congress (June 1998) <http://www.ftc.gov/reports/privacy3/toc.htm>.

70. *Id.*

71. *Supra* note 4.

72. *See* FTC, Self-Regulation and Online Privacy: A Report to Congress (July 1999) <http://www.ftc.gov/os/1999/9907/privacy99>.

follow-up on the one we did in [19]98[73]—and [at] that period of time only fourteen percent of commercial web sites had privacy statements.[74]

So there was obviously a substantial or significant improvement, but by no stretch of the imagination does that mean we are where we need to be. And the Advocates for Privacy and legislation to enforce privacy, to establish privacy protection policy and have the government monitor implementation, that movement is alive and well.

There was tremendous pressure on the Federal Trade Commission, in its report of the [19]99 survey, to make a recommendation that the government, that Congress, should start legislation for privacy.[75]

We had earlier issued a report the previous year on children's privacy.[76] And as the Professor, I think, mentioned, and perhaps someone else mentioned it earlier today, the things that are done with children, we all are in agreement, these things are just too intolerable as far as I'm concerned, and I'm sure most of you would agree, probably all.

We have a rule, as we call them in the Federal Trade Commission, that's about to be published this week, a final rule,[77] on the privacy policy that has evolved out of the Children's Privacy Protection Act[78] . . . . Complicated to put together, but the decision to put it together is an easy one.

When the privacy policy debate comes to adults, that's another issue; we are back to personal accountability and what can the government really do.

. . . .

I have been a strong advocate for, and I think for good reasons, (the position) that we should not rush to regulate something we don't fully comprehend and perhaps, more importantly, something that is virtually impossible to regulate.

I am an advocate for businesses, commercial sites, working with government and with privacy advocates, and in response to consumers' demands, to resolve this question of protecting

---

73. *See* FTC, Privacy Online: A Report to Congress (June 1998) <http://www.ftc.gov/reports/privacy3/toc.htm>.

74. *Id.*

75. *See* FTC, Self-Regulation and Online Privacy: A Report to Congress (July 1999) <http://www.ftc.gov/os/1999/9907/privacy99>.

76. *See* Prepared Statement of FTC, Protection of Children's Privacy on the World Wide Web (Sept. 1998) <http://www.ftc.gov/os/1998/9809/priva998.htm>.

77. *See* 16 C.F.R. pt. 312 <http://www.ftc.gov/os/1999/9910/64fr59888.pdf>.

78. Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (1998).

people's privacy as best as can be done.[79] I want to make that point clear.

We have laws on the book that say: "You shall not steal," but we haven't stopped stealing, I don't think. We have laws that say: "Don't commit murder," [but that] hasn't stopped murders. Our efforts, although strong, have not stopped the violations. But, in privacy, there will never be a law that will get to everyone who violates somebody's privacy. That's a fact. The technology today makes that an impossibility.

I felt that the private sector, with its technology, with its creativity, with its resources and, more importantly, with its motivation, should be able to do this better than we can do it in government.

Government doesn't do things like this very well. Number one, it takes us forever to do it. I think Jim[80] mentioned we will never catch up. He's sitting here talking about Internet 3 and all these other things—or Internet 2, I guess is what we're working on.

By the way, if you ever want to hear a fascinating discussion, ask Vinton Cerf to come out and speak to you about the Internet. He's one of the founders; contrary to what popular belief is or what they would have you believe, Vice President Gore did not invent the Internet. This guy did or was one of the several that did, and gives a fascinating presentation on what we're dealing with here, and it will boggle your mind.

"But," I said, "Let's hold off. Let's don't recommend to Congress . . . that we regulate the Internet." There was great conflict within the Commission. The chairman of the Commission and I were sort of taking the position, let's let industry keep going, we have made progress, let's enhance that, keep the pressure on, and they have all the right reasons to do it. And then there was a disagreement with the other two commissioners.

We finally issued a report that came to the right conclusion. Unfortunately, the way the FTC staff wrote it—and it was adopted by the majority, I opposed it—we talked for the first nine pages, if I remember correctly, about the [19]98 survey[81]

---

79. *See generally* Orson G. Swindle, Address to the Reston Chamber of Commerce, April 8, 1999 <http://www.ftc.gov/speeches/swindle/reston.htm>.

80. *Supra* note 4.

81. *See* FTC, Privacy Online: A Report to Congress (June 1998) <http://www.ftc.gov/reports/privacy3/toc.htm>.

which was so bad. Gave slight attention to the [19]99 survey[82] which showed some significant improvement, which industry was to be commended. It was just convoluted, but I guess due somewhat to my own insistence, we did recommend that there be no legislation at this time and to encourage industry to keep pressing on.

Industry has to keep pressing on. This is not a trivial matter, as you have seen some of the things that are captured in the way of personal information. It offends me to no end .... I was speaking to a bunch of college students in New York City a number of months ago, and we were talking about privacy on the Internet. They were a bright group of people, assembled from all over the country. I talked about privacy ... after the presentation, and I commented to a group of youngsters that I was really offended when I sign on to the *New York Times*, ... and they ask me my name and my address, and they start asking me all these questions. I just say the hell with them; I refuse to answer the questions, so I don't get to read the *New York Times*.

These youngsters laughed and said, "Don't sweat that. Give them false names and so forth." It never entered my mind to do that. You know, I'm just not up with the times, I guess. My grandmother would beat me within an inch of my life if I told somebody a lie, even on the Internet. You know, I just couldn't do that. So I've now learned how to cope with these things.

This is a serious matter; and industry, as I said, has all the right reasons to do it right. It's called "profit." Satisfied customers will keep coming back to commercial sites because they feel comfortable with what's there, the service they receive, the products they receive. Those who don't do it right are going to lose those customers.

Now, you say that will take a lot of time. It will take a lot of time. But let me give you an idea how difficult it would be for government to regulate privacy on the Internet.

There are approximately ... seventy percent of consumers who use the Internet [that] claim they do not want to make a purchase because they have no confidence in how their financial information or medical information or their personal information will be handled.[83] So that's a great red flag out

82. *See* FTC, Self-Regulation and Online Privacy: A Report to Congress (July 1999) <http://www.ftc.gov/os/1999/9907/privacy99>.

83. *See* Louis Harris & Associates and Dr. Alan F. Westin, *Commerce, Communication, and Privacy Online, A National Survey of Computer Users* (1997).

there waving in front of businesses [that] want to make a fortune on the Internet.

But, to give you an idea of just how much of a problem it would be to regulate the Internet, and privacy on the Internet, there are approximately 3.6 million commercial web sites in the United States.[84] [T]he FTC, which is a great regulator, I guess they could come to us to monitor, or we'll get [the Department of Justice] to do something on it . . . .

So, there are 3.6 million sites that we are supposed to monitor, make sure they are all copacetic, and they are doing the right thing with privacy. It's increasing at 275,000 web sites a month.[85]

Folks, it is absurd to think that government is going to solve that problem. It's going to be solved by informed consumers. It's going to be solved by good business practice, the people who want to bring in customers to buy their products and services and to be a part of their network.

And we are seeing great strides. I can recall here about two years ago, three years ago, I guess, I was living in Hawaii, and I was going to subscribe to America Online. And I got so furious with AOL because I was just being inundated with all of this spam and whatever these terms we use for the unsolicited e-mail we get. I just found it offensive. The advertisements being thrown at me left and right.

I'm on AOL now. I finally gave up and joined. You know, eventually you have to give up and go with the big guys. But I'm very pleased with AOL. The main reason I'm pleased with it, not because it's a neat little system and it does neat things, is I get very little unsolicited e-mail. They have done an amazing job of cleaning this up, and there are all sorts of software programs coming on line that will help make this better.[86] And that's all I think we can expect to do is to keep trying to improve it.

It's not unlike flying an airplane. You know, you see an airplane flying, it looks like it's smooth and everything is going wonderfully. It's not all going wonderfully. The pilot is working furiously. When you are an amateur pilot, and you are just learning, your corrections are like this, and the airplane is going

84. For extensive survey information, see <http://www.nua.ie/surveys/index.cgi>.

85. *Id.*

86. Resources available at Coalition Against Unsolicited Commercial Email <http://www.cauce.org/>.

like this. As you get better and time accumulates, the oscillations get smaller and smaller and then it's down to constant little microscopic changes that make it look smooth. I suspect solving this problem with privacy will be somewhat like that.

We have the authority at the Federal Trade Commission to pursue people who violate people's privacy, who scam them through lies and deceitful advertising. There are a lot of remedies out there, a lot of methods by which we can get at them. We will not get them all. The solution is going to be informed consumers. Forums like this, I might add, can help greatly in letting people know the problem and the solution.

I was an advocate for the private sector this past year in this argument over whether or not the Congress should legislate . . . . I have sort of gone out and fought the battle for them, and I have a good relationship with them. I'm a private sector guy, and I think this is the way we ought to do it.

Three months have gone by now since we had those hearings in Washington and, all of a sudden, privacy just sort of, poof, disappeared. Interestingly, during the heat of this, you could not pick up a paper that there was not a big article about privacy and what's the government going to do about it. The privacy advocates were just beating the drums.

One of the more interesting things about it, I think around June the 29th there was a one-day story. It was about the welfare legislation that passed a couple years ago by the Republican Congress that was going to get people off welfare. Part of that was a system whereby the government could track these deadbeat dads and make sure they came through with the monies they were supposed to provide the children. And there was some small number, thousands, tens of thousands, I'm sure, . . . of people that this database was designed to track. Lo and behold, the government was so good at this thing, they found that the program could be expanded to large populations. It has the capacity of keeping track of every single person in this room, every single person in this state, every single person in this nation. And a couple of the papers had an article on that particular day about, "Look at what the government has done." Now, you talk about an invasion of privacy, that's invasion big time. It was a one-day story. The privacy advocates who want government to get in and do something about protecting people's privacy didn't seem to be concerned about government expanding its tracking of the general population . . . .

I sent a letter last week to some of the associations of private sector, large companies that are doing some good work in this privacy matter, but they got awful silent after we killed off the effort to legislate. And I said, "Hey, guys, . . . I told you that the ability for you to self-regulate and to come up with privacy policies and practices that are responsive to the market system depends on your leadership in solving the problems.[87] We haven't solved the problems yet. We have made some progress. We must continue to make progress. Christmas is fast approaching. It's time to go out and really promote the idea of citizens being responsible, for businesses—the businesses that you all associate with, being responsible and telling people how important it is to first have sound privacy practices. Secondly, for consumers to be aware that they could lose their shirt."

Incidentally, one of the surveys that came out recently said that consumers really value their privacy, but they don't want to pay anything for it. Maybe it gets back to having the right to privacy, which I happen to agree we do, but they don't want to pay for it.

However, they will give it up for a free computer. Remember the advertisement or program here a couple months ago, free PCs. 30,000 they gave away. They got over a million applicants for these 30,000 PCs. And, to get the PC, guess what you had to do? You had to give up a lot of your privacy. You had to give them a lot of information so they could come back and beat on your brains with advertisements.

But, I went to these organizations last week with a letter and said, "Move." Because, if you don't move, there is a whole bunch of folks back here who are going to insist this time that the Congress will legislate next summer. We're supposed to look at the situation again. And, I said, we cannot prevail another year waiting for the private sector to do it unless you take the lead. It's that important.

If you are advising your clients, or you young attorneys who are about to go out in the corporate world, it's (personal privacy) important. Consumers want it. I'm not sure if they know how to demand that it be done, but that's the way the market system works, and I think, if given a chance, it will work.

87. *See generally* Orson Swindle, *An FTC Commissioner Looks at Internet Privacy*, (Nov. 1999) <http://www.ftc.gov/speeches/swindle/westin.htm>.

MR. RENZ: I think we have heard from four of the advocates now. We heard from Jim at the beginning and I'm in the process of turning it over to questions. I wonder if Jim could kind of wrap up and summarize the panel's comments . . . .

MR. HARVEY:[88] I think it's been a fascinating panel because, particularly as Professor Elison's comments indicate, privacy is something that starts from the bottom. It's a very local, individualized entity and event that will require all of us to take matters into our own hands as we participate in the Internet every day.

The FTC, the Montana Attorney General's Office, can't do everything for us. The good counsel that we get from our corporate counselors can't do everything for us. It's up to us as individuals to do something to cause the corporations to behave in an appropriate manner. I guess my question for Commissioner Swindle is, what do we do about the people that don't have privacy policies?

MR. SWINDLE: Well, you mentioned BBB Online[89] and TRUSTe.[90] We're real strong supporters of them and the programs they are trying to institute. The privacy advocates who want the legislation now aren't satisfied with the rate of progress they are making, and I contend that . . . they are in too big a rush. This again is, to use the expression I used earlier this morning, let's look before we leap on this thing . . . .

Those programs, . . . as I understand them, should be set up so there is a . . . safe harbor. It takes a bit of resources to design a privacy policy. For big corporations, it's minor bucks. Mom-and-pop operations operating a web site selling chili pepper sauce or something like that on the Internet, . . . they want to know what their customers like, they want to get this data that helps them market, they need one too. It's a little more difficult and more expensive for them to put together a privacy policy and do the things properly on the web site.

BBB Online [and] TRUSTe, as I understand it, are coming up with some sort of boilerplate privacy practice statement and methods of doing it that will receive a kind of seal of approval from us, that meets our standards. We like it; we're advocates of

88. *Supra* note 4.
89. <http://www.bbbonline.com/>.
90. <http://www.truste.org/>.

it. Online Privacy Alliance[91] is another group, . . . not doing a seal, but . . . behind some of the motivation here.

If you are the mom-and-pop operation, you say, okay, I need a privacy statement, a policy. Go copy it. Plant that sucker on your web site, and you are going to be safe harbored as long as you are adhering to the practices it advocates.

By the way, as a point of law . . . how many of you know the Geocities[92] site? If you have children, you probably know it. It's a . . . great site. They had a privacy policy stated on their site. It said, we're collecting this kind of information. If you agree to be here, we would like to know this, this and this, and we're just going to use it for our use. Guess what we found. They were selling the information to third parties. We sued them. They paid a big price for it.[93]

You can be guilty of violating your own stated, publicly stated, policies and be in big, big trouble for it. So we have the tools to go for them. The public, the consumers, need to demand good privacy practices, as well as good products and good services. I think through a combined effort of the public sector, the private sector, attorneys, [and] academics, we have got to have a discussion of this and find ways to do it as best as it can possibly be done. It will never be perfection.

91. <http://www.privacyalliance.org/>.

92. <http://geocities.yahoo.com/home/>.

93. *In the Matter of* Geocities, No. C-3850 (FTC Feb. 5, 1999) <http://www.ftc.gov/os/1999/9902/9823015d%26o.htm>.